Factoring natural numbers: Notes

1. **Definition**: a natural number \( x \) is a **factor** of the natural number \( y \), iff there is a natural number \( c \), with \( xc = y \).

2. **Definition**: a natural number is a **prime number**, iff it has exactly two factors, itself and 1.

3. **Remark**: The number 1 is NOT a prime number. (Why?)

4. Here is a list of the first few prime numbers:

   \[ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71 \]

5. Divisibility tricks: Divisible by 2 if last digit is even. Divisible by 3 if digits sum to a multiple of 3. No trick exists for 7. Trick for 11 is more complicated. Otherwise, you must divide.

6. **Theorem** (Euclid): The number of prime numbers is infinite.
   Proof: Suppose not. Then let \( Q \) = the product of all possible prime numbers. Consider \( Q+1 \).
   \( Q+1 \) cannot be divisible by any of the prime numbers, because the remainder when dividing by that prime number would be 1 (not zero). Therefore, either there is another prime not in the list of primes, that is less than \( Q+1 \), that is a factor of \( Q+1 \); or else \( Q+1 \) is itself prime. Either way, the original list of primes was not complete. So there cannot be a finite number of primes.

7. **Definition**: If a natural number \( C \) is not prime, we say it can be **factored**.

8. **Remark**: suppose \( AB = C \). Suppose \( A \leq B \). Then, either \( A < B \) or \( A = B \).

9. **Theorem**: Suppose \( C \) is a natural number. If \( C \) can be factored, then \( C \) has a factor \( A \) with \( A^2 \leq C \).
   Proof: follows from the remark above.

10. **Algorithm**: **How to factor a natural number into prime factors**:
    If \( C \) is a natural number, then we should try to divide \( C \) by each prime number less than or equal to the square root of \( C \). If one of those primes is a factor, then \( C \) can be factored. Suppose \( p_1 \) is that factor. Let \( C_1 = C/p_1 \). Then continue as before, using \( C_1 \) in place of \( C \). Continue until the result is prime. Write the result as a product of primes in ascending order, with exponents.

11. **Example**: Factor 323 into prime factors.
    We need to try the primes 2,3,5,7,11,13,17. Since \( 18^2 = 324 \) (bigger than 323), we don’t have to try any primes bigger than 17. After we divide each of these into 323, we find that \( 17(19) = 323 \). Therefore \( 323 = 17 \cdot 19 \).

12. **Example**: Factor 96 into prime factors.
    \( 96/2 = 48 \). \( 48/2 = 24 \). \( 24/2 = 12 \). \( 12/2 = 6 \). \( 6/2 = 3 \). Therefore, \( 96 = 2^5 \cdot 3 \).

13. **Example**: Factor 331 into prime factors.
    \( 19^2 = 361 \) (greater than 329), so we don’t need to try any primes bigger than 17.
    When we try the primes 2,3,5,7,11,13,17, we find that there is a non-zero remainder for each division. Therefore, \( 331 \) is a prime number.

14. **Exercise**: Factor these numbers into prime factors if possible:
    \( 12, 28, 64, 100, 132, 327, 441, 1058, 1728 \).